

HOW IT WORKS

RFID

London commuters and new passport holders already use radio frequency ID tags, and soon supermarket shoppers could follow. Tom Royal looks at the technology behind RFID, the security implications and the attempts to smash the system

Since becoming widespread in the 1980s, barcodes have revolutionised the way we shop. Rather than printing and affixing a price label to every item, which the store staff must then read at the checkout, retailers can simply associate a price with the Universal Product Code barcode printed on each item. When an item is scanned at the checkout, the till computer looks up the UPC code and adds its price to the bill.

In the near future, though, things could become quicker still. Recent advances in radio frequency identification (RFID) technology mean that queuing and unloading items on to a conveyer belt to be scanned could become a thing of the past. Instead, you'd simply push your trolley past a sensor that quickly reads the price of every item. This month we'll examine how RFID has developed, how it works and how it's currently being put to use.

FRIENDLY FIRE

RFID systems have two components: tags, which are attached to the items being monitored, and a reading device. When the tags come close to the reading device, and the device is turned on, the tags transmit information back to the reader. The range at which the system works depends on the type of RFID technology used: some work only if the tag and reader are within a few inches of one another, while others can communicate over hundreds of metres.

Transmitting information quickly and wirelessly sounds impressively futuristic, but in fact the technology behind RFID has been available for decades and was developed extensively during the Second World War. The Identification Friend or Foe system, invented at RAF Bawdsey, was designed to enable radar operators to identify which aircraft were friendly, and so should be allowed to pass unhindered, and which were enemies to be intercepted.

The system required the installation of an IFF device, fitted into an 18-inch-square box, in each RAF aircraft. Interestingly, the box had two switches: one to enable the IFF, and one to destroy it. This second switch was meant to be operated only to prevent the device falling into enemy hands, but several pilots accidentally activated the wrong switch, destroying the equipment inside in a puff of acrid smoke.

The IFF technology was a two-stage system. The ground-based radar stations would periodically emit a radio signal on a known frequency. The IFF unit in each aircraft was tuned to receive this signal and, on doing so, would emit a transmission of its own on a slightly different frequency. On receiving this signal, the ground-based radar station knew that the aircraft in question was friendly.

The IFF system is still in use today, although it has been much improved. Rather than simply receiving and sending pulses of radio waves, modern systems send and receive data. Today's military IFF systems send out a burst of coded data, which friendly aircraft match to a specific coded response that they send back. This means that enemy aircraft using the same technology will be unable to send a fake response unless they know the correct challenge and response information. IFF is used by civilian aircraft, too, with the responses used to transmit information such as the aircraft's altitude and identification.

DOWN TO EARTH

The simplest form of RFID tags work in much the same way as the IFF system, albeit on a much smaller scale. Each tag contains a radio transceiver, a battery and, occasionally, one or more sensors. Where the early IFF systems were fitted into large metal boxes, these RFID tags pack the same kind of technology into a module that can be as small as a painkiller tablet.

The tag's radio receiver listens for a signal from the reading device. When it detects this signal, it uses its radio transmitter to send information back to the reader. This information can simply be an identification number stored in its microchip controller, identifying the item to which the tag is affixed. This radio equivalent of a barcode is ideal for managing stock, so this kind of RFID tag is often affixed to shipping containers or even cattle. If the tag contains sensors, such as a temperature probe or shock detector, this information can also be transmitted to the reading device. This makes the tags useful in other fields, such as monitoring perishable items or the maturity of concrete.

This kind of RFID tag, where a battery is incorporated into the tag itself to power the transceiver and sensors, is known as an active RFID tag. Active tags cost as little as a few pounds each, and use batteries that can last as long as 10 years. They have the longest range of the various RFID systems available, and some can be read at distances of over a hundred metres.

THE PASSIVE VOICE

Active tags have many advantages, but with a battery inside they cost too much for use on relatively low-value items such as supermarket goods. Also, they're not tiny enough to be fixed unobtrusively as an anti-theft measure. The RFID tags being introduced into supermarkets and similar environments use a smaller, cheaper technology known as passive RFID.

Passive RFID tags do not require a battery, which makes them smaller and cheaper. They consist of a microchip connected to a relatively large antenna. In order to transmit a response to the reading device, the tag uses power gathered from the reading device itself. The reading device transmits a radio signal, which is essentially a sine wave, and listens for any alterations to that signal. When this signal hits the antenna built into an RFID tag, it induces a current in that antenna. This current powers up the tag's microchip.

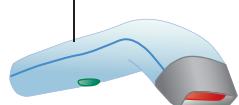
In order to send data back to the reader, the microchip temporarily passes some current back to its antenna. Driving the tag antenna in this way creates a small disturbance in the radio signal – the amplitude of the sine wave drops slightly. The reader detects this tiny drop and recognises that a tag is present.



▲ An RFID tag in new UK passports contains data about the passport holder and a digital copy of the passport photograph. Privacy campaigners have expressed concerns about the use of this technology

Waves of information How the data on an RFID tag is transmitted

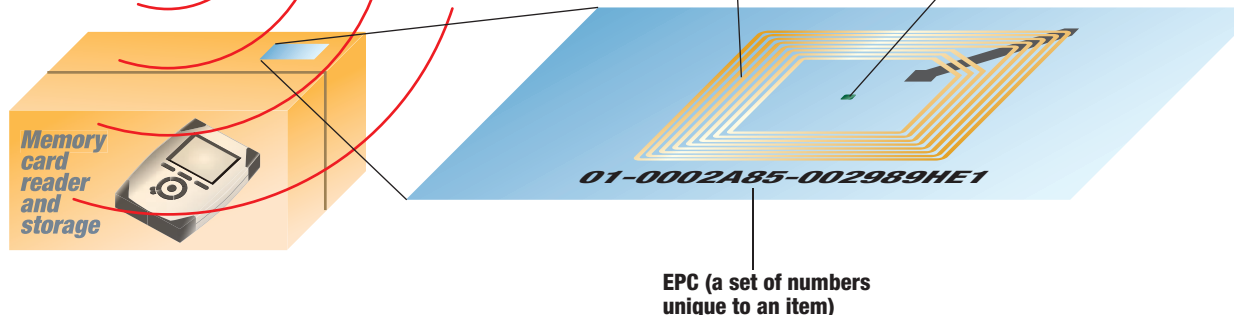
A scanner emits a radio frequency field that activates the RFID tag. It also detects the tag's disturbance to the field to decode the EPC



An antenna is incorporated into the label and responds to the scanner's signal

A microchip holds data, in this case an EPC (electronic product code)

Memory card reader and storage



EPC (a set of numbers unique to an item)

By repeatedly connecting, or shunting, its antenna, the tag can transmit binary data that the reader recognises as a series of drops in the signal amplitude. In the simplest applications, this data is a serial number identifying the item to which the tag is attached. This process of sending data back by slightly altering the radio wave connecting the two devices is known as backscatter modulation.

Passive RFID tags can be made very small. Hitachi has developed a microchip for use in tags that measures just 0.15mm by 0.15mm, and the antennas needed to gather power and transmit back to the reader can be printed on the back of a sticky label, making them an ideal substitute for barcodes. What's more, each tag can cost just a few pence each. Both Tesco and Wal-Mart have used RFID tags developed by the Smartcode corporation to protect retail goods. Passive tags have disadvantages, though. The method of transmitting data by backscatter modulation is limited to relatively short ranges, so most passive tags can be read at distances of only a few inches.

PRINTS CHARMING

Passive RFID tags are far less expensive than active tags, and they can be found in dozens of places today. New UK passports include an RFID tag that contains data about the passport holder and a digital copy of the passport photograph. It's overlaid with a clear sheet, so the chip itself and the concentric rings of wire that form its antenna are clearly visible. The Oyster cards used instead of tickets on London transport contain an RFID chip that stores details of the credit purchased by the owner. RFID chips are also used to identify pet animals, with the chip and antenna implanted under the skin, and to track and catalogue books in many libraries.

The principal problem with current RFID systems, though, remains their cost. RFID may be used in systems where the same tag is retained for a long period of time, such as a passport, or to provide protection for high-value items, but even a cost of a few pennies per tag is far greater than that of a printed barcode. In the future, though, this may not be the case.

Both Philips and PolyIC, part owned by Siemens, have demonstrated prototype RFID technology that could lead towards the mass-production of completely printed tags. The idea of printing a tag's antenna using metallic ink is not new, but the two companies have succeeded in building the tag's controller circuits using polymer-based semiconductors rather than a standard silicon-based circuit. Polymer circuits can be printed, and PolyIC claims to have created a completely printed sample RFID tag that can be read from a range of 2-3cm. If this technology can be developed further, it should be possible to print thousands of RFID tags at a relatively low cost, or even to print an integrated passive RFID tag as part of a product's packaging.

PRIVATE PRESS

It seems likely that RFID technology will continue to proliferate, but there are some concerns that could limit their use. A key problem is privacy. The idea of devices that can transmit data to a remote person without their owner's knowledge is disconcerting, and as some RFID devices have a long range, there is potential for tags to be read by a third party. This is particularly troubling when the devices contain important personal information, such as passports.

The information contained in the RFID chip of a current UK passport is encrypted using the triple DES, or 3DES, algorithm. 3DES is considered secure because the time required to break it using brute force is currently prohibitive, but this assumes that the snooper doesn't know the key in the first place.

In fact, the key used to secure biometric passports is generated from the passport number, the owner's date of birth and the passport expiry date. This data is printed on the passport in a computer-readable format. The idea is that the immigration official can swipe this data into his computer, then use it to access the RFID chip. Someone lurking across the hall from the passport would not have access to the passport information, so he could not unlock the RFID chip's information.

Some have argued that this system makes it easy for someone in possession of the passport

for even a minute or so to read the RFID chip's contents and create a fake passport with a cloned chip. Anyone with access to public records could find out at least part of the key.

Other concerns have been raised about the potential use of RFID tags on low-cost consumer goods. Groups such as Consumers Against Supermarket Privacy and Numbering (or CASPIAN), which previously campaigned against store loyalty cards, have complained that the tags are in effect 'spy chips' that supermarkets can use to invade the privacy of consumers. CASPIAN has also campaigned against the VeriChip human RFID implant, publicising information filed in the company's S-1 stock exchange registration statement. This identifies "potential or perceived" risks to health that include "adverse tissue reactions, migration of the microchip and infection from implantation".

This opposition to RFID has even resulted in devices designed to destroy passive RFID tags. One group of engineers has demonstrated a method that lets you convert the flash unit in a disposable film camera to emit a pulse of radio waves. This induces too much current in the antenna of any passive RFID tags placed nearby, damaging the microchip and rendering the tag useless. A simpler method for destroying most RFID tags is to disconnect the antenna. **CS**

FURTHER INFORMATION

The history of the Identification Friend or Foe system:
<http://jproc.ca/sari/sariff.html>

Backscatter modulation explained
<http://www1.microchip.com/downloads/en/appnotes/00680b.pdf>

How to break into a UK passport's RFID information:
www.guardian.co.uk/identity/story/0,,1950226,00.html

Consumer campaign against RFID tags:
www.spychips.com

VeriChip's S-1 statement:
www.sec.gov/Archives/edgar/data/1347022/000119312507024937/ds1a.htm